Manage Vulnerabilities (VULN) Capability Data Sheet

Desired State:

- Software products installed on all devices are free of known vulnerabilities [1]
- The list of known vulnerabilities is up-to-date

Desired State Data Requirements:

Data Item	Justification
Authorized Hardware Inventory	To identify what devices to check
The associated Value for every device attribute[2]	To prioritize defects associated with devices.
A version controlled and dated listing of all software products that have at least one known vulnerability to include: • Vulnerable software product in same format as the Authorized Software Inventory (CPE or SWID equivalent) • All CVEs associated with that software product For every locally defined[3] known vulnerability maintain a version controlled and dated listing to include: • Vulnerable software product in same format as the Authorized Software Inventory (CPE or SWID equivalent) • Identifier of all local vulnerabilities associated with that software product • Severity for each local vulnerability (CVSS score equivalent)	To detect known vulnerabilities present on the system

[1] Often it is not feasible to have no known vulnerabilities present (e.g., patch is not yet available), so the goal is to minimize their presence in the environment.
[2] This value will initially be defined by the D/A for the SWAM capbility. Once the necessary data becomes available, it will be calculated from the value assigned by the D/A to assets.

Data Item	Justification
Alternative mitigation specification[4] for any known vulnerability where the source vendor provides a mitigation option that can be implemented instead of patching/reversioning the software to include: • CVE or local identifier • Associated system attributes • Required/acceptable values • Compliance definition	To exclude vulnerabilities mitigated by alternative methods that can be automatically checked[5] from the score To determine compliance with each specific check

Actual State:

- Listing of all enumerated vulnerable software installed on all devices
- All CVEs on all devices that are appropriately mitigated by alternative methods
- Collection mechanisms and/or processes to detect and record/report the Actual State information

Actual State Data Requirements:

While not explicitly stated below, all Actual State Data elements must have a date/time associated with each collection instance of that element[6].

Data Item	Justification
The vulnerable software installed on every device.	To identify defects
Devices that are compliant with alternative mitigation specifications to include the CVEs or local identifiers that are appropriately mitigated	To eliminate those vulnerabilities from the score

[3] Departments and Agencies can define data requirements and associated defects for their local environment. This is done in coordination with the CMaaS contractor and these local defects are not reported to the Federal Dashboard.

[4] Some known vulnerabilities can be equivalently mitigated by not installing sections of code, executables, or via configuration options.

[5] If the check that determines implementation of the alternative mitigation method can be verified by checking registry settings, executable hashes, or configuration settings, then a specification can be defined to automatically determine that the vulnerability is not present.

[6] Collection often occurs in batches, where the sensors collect from a set of devices at once. As long as a date/time can be provided for the data resulting from that collection to a reasonable precision (i.e., ± 1 hour), that is acceptable.

Data Item	Justification
Data necessary to determine how long vulnerable software has been present on a device. At a minimum: • Date/time it was first discovered • Date/time it was last seen	To determine how long vulnerabilities have been present on a device

Defects:

A defect is the existence of an installed software product that contains at least one known vulnerability or using out-dated/incomplete CVE data. The following are the defects for VULN:

Defect Type:	Why is this considered a risk condition?	Typical Mitigation[7] Option 1:	Typical Mitigation Option 2:
Device has vulnerable software product installed	Device is vulnerable to exploitation	Apply patch or upgrade software product	Otherwise, remove software product from the device
Vulnerable software listing does not contain up to date CVE or local vulnerability data	Device is vulnerable to exploitation but reported that it is not or scores do not adequately reflect risk	Update the listing and implement process to perform timely updating	Otherwise, remediate the implementation issue with existing process
An important data element of the vulnerable software listing or alternative mitigation specificiation is missing	A key piece of information used to score risk is unknown	If the data element is known, record the information	Otherwise, determine or define the data element and record the information
Vulnerable software can not be reported within a set timeframe for a device (Non-reporting for Vulnerabilities)	The Department or Agency's (D/A) ability to monitor vulnerabilities is limited	Work with the sensor/collection managers or process owners to troubleshoot/resolve the problem.	Otherwise, revoke or suspend the device's authorization

[7] Risk acceptance is always an option. In the case of Option 1 and Option 2, the risk conditions and scores do not go away. They remain visible to ensure that the D/A understands the impact of their risk acceptance decisions over time and in aggregate.

Appendix A - Definitions

Term	Definition
Authorized Hardware Inventory List	List of authorized hardware assets for an organization or subnet.
Authorized Software Inventory	Managed software whitelists and blacklists for the organization and each device attribute.
Blacklist	List of unauthorized software for a D/A or device.
Common Platform Enumeration (CPE)	Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.[8]
Common Vulnerabilities and Exposures (CVE)	Common Vulnerabilities and Exposures (CVE) is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems.[9]
Common Vulnerability Scoring System (CVSS)	CVSS measures the severity of a vulnerability compared to other vulnerabilities so remediation efforts can be prioritized.
Compliance Definition	The logic associated with a check that expresses how to determine if an asset is compliant with the policy.
Defect	A condition where the Desired State specification and the Actual State do not match in a manner that incurs risk to the organization.
Device	IP-addressable asset on the network or a non-addressable component (e.g. removable media) able to interact with the D/A's data and resources.
Device Attribute	Device attributes are a way to describe a set of labels, values, and hierarchies associated with dimensions or characteristics of a device. The attributes assigned to a device are used to determine the applicability of a defect check, the result domain of a defect check, or create the appropriate desired state specification for a defect check associated with that device.
Manage Vulnerabilities (VULN) Capability	This capability is to ensure that vulnerabilities are identified and removed or remediated from devices to minimize exploitation.

[8] http://nvd.nist.gov/cpe.cfm

[9] http://cve.mitre.org/about/faqs.html#a1

Term	**Definition**
National Vulnerability Database (NVD)	NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.[10]
Scoring	The process of calculating the risk points for a defect. Identified defects will be "scored" based on the amount of perceived risk they create. The CDM program will be providing a scoring system that is generic across D/As. Each D/A may adapt this with additional D/A specific information to better prioritize defects for action.
Software Asset Management (SWAM) capability	The CDM capability that ensures unauthorized and/or unmanaged software is 1) identified, 2) authorized, and 3) assigned for management, or 4) removed before it can be exploited compromising confidentiality, integrity, and availability.
Software identification tag (SWID)	Software ID tags provide authoritative identifying information for installed software or other licensable item.[11]
Software product	The level of abstraction by which software is typically licensed, listed in registries during installation, and executed by users. Software products are roughly equivalent to the software identified by the NIST Common Product Enumeration (CPE) codes, and also by the ISO SWIDs.
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Whitelist	List of authorized software for a D/A or device.

[10] http://nvd.nist.gov/

[11] ISO/IEC 19770-2: Software identification tag